



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ML

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/883,371	06/19/2001	Shuji Shichi	PNDF-01078	1070
466	7590	01/19/2007	EXAMINER	
YOUNG & THOMPSON 745 SOUTH 23RD STREET 2ND FLOOR ARLINGTON, VA 22202			DASS, HARISH T	
			ART UNIT	PAPER NUMBER
			3693	
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE		
3 MONTHS	01/19/2007	PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/883,371	SHICHI, SHUJI	
	Examiner	Art Unit	
	Harish T. Dass	3693	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on ____.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 16-35 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) Claim(s) ____ is/are allowed.
- 6) Claim(s) 16-35 is/are rejected.
- 7) Claim(s) ____ is/are objected to.
- 8) Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on ____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. ____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date: ____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date: ____	6) <input type="checkbox"/> Other: ____

DETAILED ACTION

The finality of the previous Office action has been withdrawn based on applicant's filed paper 12/07/07.

Claims 1-15 are cancelled.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 16-35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Independent claims 16 and 30 limitation "a different user-input password number and a different current password number is required for each of plural transactions" is not clear. How do "a different user-input password and a different current password number is required for each plural transactions" and "a different user-input password and a different current password is required for each validation of the card" work by putting two different password that are not in the database to be validated. Provide portion of specification which describes the feature.

Claims 16-35 rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted step is: How "a different user-input password and a

different user-input password" are validated, and they are different than which passwords respectably.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 16-21 and 30-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over KWAN (US 2003/0200179) in view of Novoa et al. (hereinafter Novoa –US 6,636,973) and Khello (WO 97/11443).

Re. Claim 16, KWAN discloses providing a user with a prepaid card linked to a database [para. 20]; and

executing an action chain including validating the prepaid card by comparing a user-input password number, input by the user, with a current password number stored in the database [claim 5; para 0021], and after the first validation of the prepaid card, validation of the prepaid card requires successful comparison of a currently user input password number to the stored current password number [see claim 5].

KWAN does not explicitly disclose wherein, a different user-input password number and a different current password number is required for each of plural transactions, a first validation of the prepaid card uses a system-set first-time password

Art Unit: 3693

number stored on the database as the current password number, after each validation, the user sets a new user-set password number as the current password number stored in the database.

However, validation of passwords and changing the passwords are well known to protect unauthorized use of computer accounts, credit cards, and debit cards, where the user must input the active password and new password in order to change the active password to new password (which will be a new active password for next login), and omitting either of the passwords (active and new) does not change the password.

Novoa a first validation of the prepaid card uses a system-set first-time password number stored on the database as the current password number, after each validation, the user sets a new user-set password number as the current password number stored in the database [col. 2 lines 27-49; col. 3 lines 6-25] to increase the security for unauthorized access to the accounts (computer accounts, debit card, smart card, pre-paid card, etc). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of KWAN and include a first validation of the prepaid card uses a system-set first-time password number stored on the database as the current password number, as disclosed by Novoa, to compare user's id and an active user password inputted by the user with database stored record for validation of the user, before letting the user to change the password that is stored in the database. KWAN or Novoa does not explicitly disclose a different user-input password number and a different current password number is required for each of plural transactions. Khello discloses this feature [page 2 line 26 to page 3 line 9] to provide a user authentication service that offers a high level of security. It would have been

obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of KWAN and Novoa and include a different user-input password number and a different current password number is required for each of plural transactions, as disclosed by Khello, to provide a short term user input password to be changed each time a service is requested for security and protection of the user's card/account.

Re. Claim 17, KWAN discloses wherein the prepaid card is a virtual card [para 09; 05; 18].

Re. Claim 18, KWAN discloses the prepaid card comprises a physical card carrying duplicate information carried in the database, the prepaid card comprises a serial number, the first-time password number, and an expiration date printed on an exterior surface of the physical card, and the database comprises the serial number, the first-time password number, and the expiration date of the prepaid card [Figure 1; para 21; 63; claim 1]

Re. Claim 19, KWAN discloses the first-time password number is concealed below of scratch-off covering [Figure 5; para 21].

Re. Claim 20 KWAN discloses the database includes a database record corresponding to the prepaid card and comprising a serial number field storing a system-assigned serial number, a first-time password number field storing the system-assigned first-time

password number used for a first time validation of the prepaid card, and a user-set password number field for storing the user-set password number reset as the current password number by the user subsequent to each validation of the prepaid card, a monetary balance field storing a monetary balance available to the user [Figures 2-3; para 19-21; claim 8;], and comprising the further step of: subsequent to the validation of the prepaid card, a action of subtracting a price being necessary for distribution from monetary balance field to update the monetary balance field by reducing a value of the monetary balance field by the price being subtracted [para 21; 32-35; claim 5].

Re. Claim 21 KWAN discloses an issue date field, an expiration date field, a card monetary face value field, a transaction product/service number field , and a transaction date field, each having a one-to-one correspondence with the prepaid card [Figures 4-5; para 75; 93; 69].

Re. Claim 30, KWAN discloses executing an action chain including validating a user's card by comparing a user-input password with a current password stored in a database [claim 5; para 0021], and a first validation of the card uses a system-set first-time password stored on the database as the current password [para. 19-21]. KWAN does not explicitly disclose wherein, a different user-input password and a different current password is required for each validation of the card, and after each validation, the user sets a new user-set password as the current password stored in the database, and after the first validation of the card, subsequent validation of the card requires successful comparison of a currently input user input password to the stored current password in

the database. However, validation of passwords and changing the passwords are well known to protect unauthorized use of computer accounts, credit cards, and debit cards, where the user must input the active password and new password in order to change the active password to new password (which will be a new active password), and omitting either of the passwords (active and new) does not change the password.

Novoa discloses after each validation, the user sets a new user-set password as the current password stored in the database, and after the first validation of the card, subsequent validation of the card requires successful comparison of a currently input user input password to the stored current password in the database [Figures 3-4; col. 8 lines 18-56] to increase the security for unauthorized access to the account.

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of KWAN and include a first validation of the prepaid card uses a system-set first-time password number stored on the database as the current password number, as disclosed by Novoa, to compare user's id and an active user password inputted by the user with database stored record for validation of the user, before letting the user to change the password that is stored in the database. KWAN or Novoa does not explicitly disclose a different user-input password and a different current password is required for each validation of the card (every service transaction). Khello discloses this feature [page 2 line 26 to page 3 line 9] to provide a user authentication service that offers a high level of security. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of KWAN and Novoa and include a different user-input password number and a different current password number is required for each of transaction, as

disclosed by Khello, to provide a short term user input password to be changed each time a service is requested for security and protection of the user's card/account.

Re. Claim 31, KWAN discloses the card comprises a physical card carrying duplicate information carried in the database [Figure 1; para 21; 63; claim 1], and the card each comprises a serial number, the first-time password number, and an expiration date printed on an exterior surface of the physical card [Figure 1; para 21; 63; claims 1 & 4].

Re. Claim 32, KWAN discloses the database includes a database record corresponding to the card and comprising a serial number field storing a system-assigned serial number, a first-time password field storing the system-assigned first-time password used for a first time validation of the card, and a user-set password field for storing the user-set password reset as the current password number by the user subsequent to each validation of the card, a monetary balance field storing a monetary balance available to the user, and comprising the further step of: subsequent to the validation of the card, a action of subtracting a transaction' price for distribution to a vendor from the monetary balance field to update the monetary balance field by reducing a value of the monetary balance field by the price being subtracted [Figures 2-3; para 19-21; 32-35; claims 5 & 8].

Re. Claim 21 KWAN discloses an issue date field, an expiration date field, a card monetary face value field, a transaction product/service number field, and a transaction

date field, each having a one-to-one correspondence with the card [Figures 4-5; para 75; 93; 69].

Re. Claims 34-35, Novoa further discloses a portal site, located between a user and the database, receiving from the user an input of the card serial number and the currently user input password; the portal accessing the database and validating the card by comparing the received user-input password with the current password stored on the database, and after validation of the card, the portal site i) requests the user to input the new user-set password, ii) receives the new user-set password from the user, iii) sends the received new user-set password to the database to be stored, in the user-set password field, as the current password required for a next validation of the card [Abstract; col. 2 lines 27-49; col. 3 lines 6-25] to increase the security for unauthorized access to the account since the current pre-paid card have code printed on them and any one can use it if the card is lost or stolen. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosures of Kwan, Novoa, Khello and Rubin and include provisioning for the user to reset password for enhancing the security of the pre-paid card and storing the new password in database for validation of the card to prevent fraud and misuse of the customer pre-paid account.

Claim 22-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over KWAN and Novoa and Khello as it applied to claims 16 and 20 above, further in view of Rubin et al (hereinafter Rubin – US 6,701,522).

Re. Claims 22-24, KWAN discloses located between a user and the database, receiving from the user an input of the card serial number and the currently user input password number; the portal accessing the database and validating the prepaid card by comparing the received user-input password number with the current password number stored on the database [claim 1], and wherein the portal site is connected to the user and to the database via the Internet and wherein the portal site is connected to the user via a telephone line and (see use of internet and telephone for activation) [para. 60; claim 1]. KWAN, Novoa or Khello does not explicitly disclose portal, or a portal site. However, Rubin discloses this feature [see Abstract; Figures 1-2, 7; col. 1 lines 5-50] to allow a user(s) (purchaser) to customize interested websites, which will be automatically retrieved and display information the user is seeking. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of KWAN, Novoa and Khello and include portal, as disclosed by Rubin, to allow the user to configure its favorites website for obtaining information or purchases.

Re. Claim 25, KWAN discloses wherein the user orally inputs the password number to the portal [para. 60].

Re. Claim 26, KWAN, Novoa, Khello or Rubin does not explicitly disclose the portal site further receives user input of the serial number and confirms the expiration date of the prepaid card to the database prior to validating the prepaid card. However, this function is well known function of using credit cards. For example, when a customer orders a product online or by phone the merchant asks these question to properly charge the customer as-will-as validates the card. It would have been obvious at the time the invention was made to a person having ordinary skill in the art to modify the disclosure of Kwan, Khello, Novoa and Rubin and include this function to enhance the security of the card in case it is used improperly.

Re. Claims 27-28, Novoa further discloses after validation of the prepaid card, the portal site i) requests the user to input the new user-set password number, ii) receives the new user-set password number from the user, iii) sends the received new user-set password number to the database to be stored, in the user-set password number field, as the current password number required for a next validation of the prepaid card and a next successful validation of the prepaid card requires the portal site i) to receive from the user another password number input, 'and ii) to successfully compare the received another password number input with the current password number stored in the user-set password number field of the record of the prepaid card within the database. However Novoa discloses these features [Abstract; col. 2 lines 27-49; col. 3 lines 6-25] to increase the security for unauthorized access to the account since the current pre-paid card have code printed on them and any one can use it if the card is lost or stolen. It would have been obvious at the time the invention was made to a person

having ordinary skill in the art to modify the disclosures of Kwan, Novoa, Khello and Rubin and include provisioning for the user to reset password for enhancing the security of the pre-paid card and storing the new password in database for validation of the card to prevent fraud and misuse of the customer pre-paid account.

Re. Claim 29, KWAN discloses wherein the user orally inputs the password number to the portal site and the portal site orally responds to the user, via a telephone call [para. 60].

Response to Arguments

3. Applicant's arguments with respect to pending claims have been considered but are moot in view of the new ground(s) of rejection and the followings:

In response to applicant's arguments, the recitation (*page 10 of remarks*) "neither of KWAN and RUBIN teaches the ... concept of settling ..." has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). Also see *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's argument recitation "*validation of pre-paid card*", KWAN discloses this step in claim 5 (see claim 5) "means for identifying the pre-paid card account based on the activation information and means for prompting the user to enter the security information; means for collecting the security information code, and means for verifying the security information code is correct for the particular pre-paid card; means for prompting the user to enter a user identifier if the user has an account; means for collecting the user identifier; means for identifying the user based on the user identifier and means for prompting the user to enter a password identification code; means for collecting the password identification code, and means for verifying the password identification code is correct for the user".

In response to Applicant's remaining argument, applicant is directed to the specification pages 7-9, which described the limitations of independent claims and the following responses. Note: Application is a translation of foreign application and in order to understand the limitations, examiner has to relay's on the specification pages 7-9 (Actions 1-16).

- I. *Secondary reference Novoa et al. (or Novoa - US 6,636,973), discloses the validation and change of password (not only biometric but conventional username/password) before accessing the secure web page as described in applicant's specification page 7-9 [see col. 1 lines 24-40; col. 2 lines 29-32 "most computer systems ... data entry method."; col. 2 lines 50-57 "dynamically changes a user's password preferably each time the user ... database that contains a password, username (optional); col. 3 lines 15-22 "at some*

point during or after the log on process ... not require to remember and type the password."; col. 3 lines 31-35 "Further, in one embodiment, the newly generated ... In an alternative ... next time the user attempts to log in."; col. 8 line 57 to col. 9 line 5 "An alternative ... dynamically changing the user's password during log on ... client 208"].

Further,

II. Emails websites such as Yahoo.com, att.net (attworldnet.net in 1996), hotmail.com, or etc. are well known to registered users of these services.

In order for a user to register with these website for email service, the user must create a user ID and password during registration and in order to check his/her email, the user must input his/her valid username (id or card number) and valid password (pin or PID) to obtain the secure site and check his/her email. These are the same steps that the applicant's specification has described in pages 7-8 (Action 1, through Action 8 and part of Action 9), where the username is permitted to access the secure site. These steps are needed every time the user check his/her email.

Once the user has access to the secure webpage, he/she is asked to if he/she wants to change password (optional in Yahoo.com), applicant's Actions 9-15. It is obvious that user must have his/her username/password in system's database for future authentication; otherwise system does not let him/her to log in. Once a person is logged, than he/she can conduct business until he/she logs-off.

III. It is well known one ordinary skill in the art and a user of Secure network (Intranet), Unix, MSNetwork, etc., when an account is opened, of user, an administrator creates a

user id and temporary password. The user is asked to change his/her password and when the user changes his/her password, the new password associated with user id is stored in active directory database for future log in and authentication. Every time the user is login to the system he/she require to input the user id and password and the password is a temporary password with expiration period selected by the system administrator. The user can change his/her password to new password and time. In event the user does not want to change his/her password and password time is about to expire, the system warns the user to change his/his password before it expires and before accessing the secure site. These are the same steps described in the applicant's specification (Action 1 through Action 15).

It should be pointed out that the password expiration time depended on the system administrator's choice (business), to setup of 15 days, 3 months, etc. or dynamic RSA SecurID token (every minute). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to change his/her password in event the password is lost (compromised) or about to expire, he/she has to change the old password with new password.

IV. It is well known one ordinary skill in the art and a user of Secure network (Intranet), Unix, MSNetwork, etc., in case user forgets his/her password/user id, the system administrator assigns the user a temporary password, which will be changed once the user access the system.

In response to applicant's argument that Novoa is nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention.

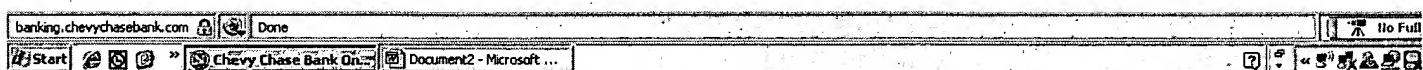
See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, username and password of Novoa is same as applicant's pre-paid card number (serial number) and PIN (password).

Note; it should be pointed out that settlement of credit card, or prepaid card is inherent in disclosure of Kwan's. Pre-paid cards are known, such as phone card with original pin printed on them, where the cards are paid during purchase. Another types of card which is settled immediately is smart card that has money purse in the card and the card is protected by a password.

The following web page is from Chevy Chase Bank which shows that to change a password requires current password and new password. This is known feature for changing password.

Art Unit: 3693

The screenshot shows a Netscape browser window for Chevy Chase Bank Online Banking. The URL in the address bar is <https://banking.chevychasebank.com/cgi-bin/Banking/2/pref/changePassword.jsp>. The page title is "Preferences - Change Password". The left sidebar has a "Main Menu" with options like "Account Info", "Transfers", "Bill Payment", "Preferences" (which is selected), "Balance Summary", "Set-up Account Preferences", "Add/Modify Balance Alerts", "e-Statement Alerts", "Manage Custom Views", "Update My Profile", and "Change Password". The main content area has a form titled "Complete the following to change your password." It contains fields for "Current Password", "New Password", and "Confirm New Password". Below the form are "Continue" and "Cancel" buttons. A link "Tips on selecting a password." is also present.



In Chevy Chase Bank, once an account holder login to secure site, he/she can pay as many bills as he/she wishes until log-off.

Conclusion

Claims 16-35 are pending and this office action is made non-final.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harish T. Dass whose telephone number is 571-272-6793. The examiner can normally be reached on 8:00 AM to 4:50 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James A. Kramer can be reached on 571-272-6783. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Harish T Dass
Examiner
Art Unit 3693



01/16/2007